**Amendments to the Claims:**

Please replace all prior versions, and listings of claims in the application with the following listing of claims.

**Listing of claims**

Claim 1 (currently amended): A method of encrypting communications from a computer having an application program interface, the method comprising:

initiating communications from said computer over a computer network;

determining that encryption of said communications is required;

establishing a connection with ~~using~~ a mobile communications device, ~~which~~ wherein said mobile communications device includes a cryptographic module for use in mobile communication over a wireless communications network; and

using the cryptographic module of the mobile communications device[[,]] as a cryptographic service provider for encrypting said communications from said computer over said computer network without sending said encrypted communications over said wireless communications network.

Claim 2 (original): A method as claimed in claim 1, wherein the mobile communications device is a WAP-enabled device.

Claim 3 (original): A method as claimed in claim 1, wherein the cryptographic module is that used by the mobile communications device for Wireless Transport Layer Security communications.

Claim 4 (currently amended): A method as claimed in claim 1, ~~comprising providing~~ wherein the step of establishing a connection with the mobile communications device comprises establishing a wired connection between the mobile communications device and the computer.

Claim 5 (currently amended): A method as claimed in claim 1, ~~comprising providing~~ wherein the step of establishing a connection with the mobile communications device comprises

establishing a wireless connection between the mobile communications device and the computer.

Claim 6 (original): A method as claimed in claim 1, comprising:

when the application program interface requires cryptographic functionality, calling a cryptographic service provider function in the mobile communications device.

Claim 7 (currently amended): A mobile communications device, comprising:

means for communicating over a wireless interface with a wireless communications network;

means for connection to a remote computer without involving the wireless communications network; and

a cryptographic module, the cryptographic module being usable:

for encoding wireless communications from the device over said wireless interface;

[[in]] by a cryptographic service provider with an application program interface of [[a]] the remote computer.

Claim 8 (currently amended): A mobile communications device as claimed in claim 7, ~~having~~ wherein the means for connection to the remote computer comprises a short-range wireless communications transceiver, for sending signals to and receiving signals from the remote computer.

Claim 9 (currently amended): A mobile communications device as claimed in claim [[7]] 8, wherein the short-range wireless communications transceiver uses Bluetooth wireless technology.

Claim 10 (original): A mobile communications device as claimed in claim 7, wherein the cryptographic module is usable to support wireless communications using Wireless Transport Layer Security.

Claim 11 (original): A mobile communications device as claimed in claim 7, wherein the cryptographic module uses public key cryptography.

Claim 12 (original): A mobile communications device as claimed in claim 7, comprising means for sending and transmitting data using WAP.

Claim 13 (original): A mobile communications device as claimed in claim 7, wherein the cryptographic module is realized in hardware in the device.

Claim 14 (original): A mobile communications device as claimed in claim 7, wherein the cryptographic module is realized in software in the device.

Claim 15 (original): A mobile communications device as claimed in claim 7, wherein the cryptographic module is provided on an external smart card.

Claim 16 (original): A mobile communications device as claimed in claim 7, wherein the cryptographic module comprises a Wireless Identity Module card.

Claim 17 (original): A mobile communications device as claimed in claim 16, wherein the cryptographic module comprises a Wireless Identity Module card which allows communications using Wireless Transport Layer Security.

Claim 18 (original): A mobile communications device as claimed in claim 7, comprising an interface for receiving a command from a personal computer, the mobile communications device acting as a cryptographic service provider for said personal computer in response to said command.

Claim 19 (currently amended): A tangible module for a personal computer, wherein, in response to the module receiving a first command from a cryptographic application program interface, indicating that it requires cryptographic functionality for communication over a computer network, the module sends a second command to a mobile communication device, the mobile communication device having a cryptographic module for use in mobile

communication over a wireless communications network, such that the ~~mobile communications device~~ cryptographic module acts as a cryptographic service provider for said personal computer allowing the personal computer to communicate encrypted data over said computer network without sending data over said wireless communications network.

Claims 20-23 (canceled)

Claim 24 (currently amended): A ~~computer~~ system, comprising:

a computer; and

a mobile communications device, including a cryptographic module for performing cryptographic functions in mobile communication over a wireless communications network,

the computer having at least one application which requires cryptographic functionality for communication over a computer network,

a first part of the required cryptographic functionality being provided in the computer, and a second part of the required cryptographic functionality being provided in the mobile communications device,

the computer and the mobile communications device having means for establishing a secure communications path therebetween; and

the computer further comprising an interface device which, on determining that an application needs to use cryptographic functionality, selects the functionality provided in the computer, or the functionality provided in the mobile communications device, and sends a command thereto.

Claim 25 (original): A computer system as claimed in claim 24, wherein the mobile communications device is a WAP-enabled device.

Claim 26 (original): A computer system as claimed in claim 24, wherein the computer application which requires cryptographic functionality is an internal memory access application.

Claim 27 (original): A computer system as claimed in claim 24, wherein the computer application which requires cryptographic functionality is an external communication application.

Claim 28 (currently amended): A method of ~~providing cryptographic functionality in~~ encrypting communications from a computer having ~~a cryptographic~~ an application program interface, wherein the communications are over a computer network, the method comprising:

~~using~~ sending data to be encrypted from the computer to a mobile communications device, ~~which includes~~ wherein the mobile communications device has a cryptographic module for ~~use in mobile communication, to provide the cryptographic functionality~~ performing cryptographic functions in communications over a wireless communications network, and further, wherein the mobile communications device uses the cryptographic module to encrypt the data;

receiving encrypted data at the computer from the mobile communications device; and

using the encrypted data in communications over the computer network without sending the encrypted data over the wireless communications network.

Claim 29 (original): A method as claimed in claim 28, wherein the mobile communications device is a WAP-enabled device.

Claim 30 (original): A method as claimed in claim 28, wherein the cryptographic module is that used by the mobile communications device for Wireless Transport Layer Security communications.

Claim 31 (canceled)

Claim 32 (original): A method as claimed in claim 28, comprising using a cryptographic module realized in hardware in the mobile communications device.

Claim 33 (original): A method as claimed in claim 28, comprising using a cryptographic module realized in software in the mobile communications device.

Claim 34 (original): A method as claimed in claim 28, comprising using a cryptographic module provided on an external smart card which can be read by the mobile communications device.

Claim 35 (original): A method as claimed in claim 28, comprising using a cryptographic module provided on a Wireless Identity Module card in said mobile communications device.

Claim 36 (currently amended): A ~~computer~~ system for supporting an application, the ~~computer~~ system comprising:

a computer including:

a cryptographic application program interface; and

a cryptography service provider; and

a mobile communication device including a cryptographic module,

wherein, when the cryptographic application program interface determines that the application requires cryptographic functionality for communication over a computer network, the cryptographic application program interface sends a command to the cryptography service provider, and

wherein the cryptography service provider has a communications link to [[a]] the cryptographic module of [[a]] the mobile communications device, the cryptographic module of the mobile communications device being usable to encrypt communications between the mobile communications device and a telecommunications network over a wireless interface, and

wherein the cryptography service provider can obtain the cryptographic functionality, required by the application, from the cryptographic module of the mobile communications device without the mobile communications device sending the encrypted communications over the telecommunications network.

Claim 37 (original): A system as claimed in claim 36, wherein the cryptographic module is realized in hardware in the mobile communications device.

Claim 38 (original): A system as claimed in claim 36, wherein the cryptographic module is realized in software in the mobile communications device.

Claim 39 (original): A system as claimed in claim 36, wherein the cryptographic module is provided on an external smart card which can be read by the mobile communications device.

Claim 40 (original): A system as claimed in claim 36, wherein the cryptographic module is provided on a Wireless Identity Module card in said mobile communications device.

Claim 41 (original): A system as claimed in claim 36, wherein the cryptography service provider has a Bluetooth wireless communications link to the mobile communications device.

Claim 42 (original): A system as claimed in claim 36, wherein the cryptography service provider has some cryptographic functionality, and, on receipt of a command from the cryptographic application program interface, determines whether it can perform the required cryptographic functionality, or whether to obtain the required cryptographic functionality from the cryptographic module of the mobile communications device.

Claim 43 (original): A system as claimed in claim 36, wherein the communications link between the cryptography service provider and the cryptographic module of the mobile communications device uses a command set defined in a standard PKCS#11, where the commands are redefined as AT commands.

Claim 44 (currently amended): A mobile communications device, the mobile communications device being able to communicate over a first wireless interface with a telecommunications network, and comprising a cryptographic module to provide cryptographic functionality for use in communications over the first wireless interface, the mobile communications device further comprising a security manager module for receiving commands from a computer system over a second interface, wherein, in response to suitable commands received from the computer system over the second interface, the security manager module requests a cryptographic function from the cryptographic module, and returns the results of the cryptographic function to the computer system over the second

interface, without sending the results of the cryptographic function over the first wireless interface.

Claim 45 (original): A mobile communications device as claimed in claim 44, wherein the security manager module responds to a command set defined in a standard PKCS#11, where the commands are redefined as AT commands.

Claim 46 (original): A mobile communications device as claimed in claim 44, wherein the second interface is a Bluetooth short-range radio interface.

Claim 47 (original): A module for a computer system, the module comprising:

an application interface for connection to a computer application; and

an external interface for connection to a mobile communication device containing a cryptographic module;

wherein, when the module receives from the application interface a request for a cryptographic function which the module is unable to provide, the module sends a command over the external interface to the mobile communications device to request the cryptographic function therefrom.

Claim 48 (currently amended): A module for a computer system as claimed in claim 47, wherein the module has some cryptographic functionality, and comprises means for determining in response to a request from the application interface whether it is able to provide the requested ~~function~~ cryptographic function.

Claim 49 (original): A module for a computer system as claimed in claim 47, wherein the external interface is a Bluetooth short-range radio interface.

Claim 50 (original): A module for a computer system as claimed in claim 47, wherein the module sends over the external interface a command from a command set as defined in a standard PKCS#11, where the commands are redefined as AT commands.